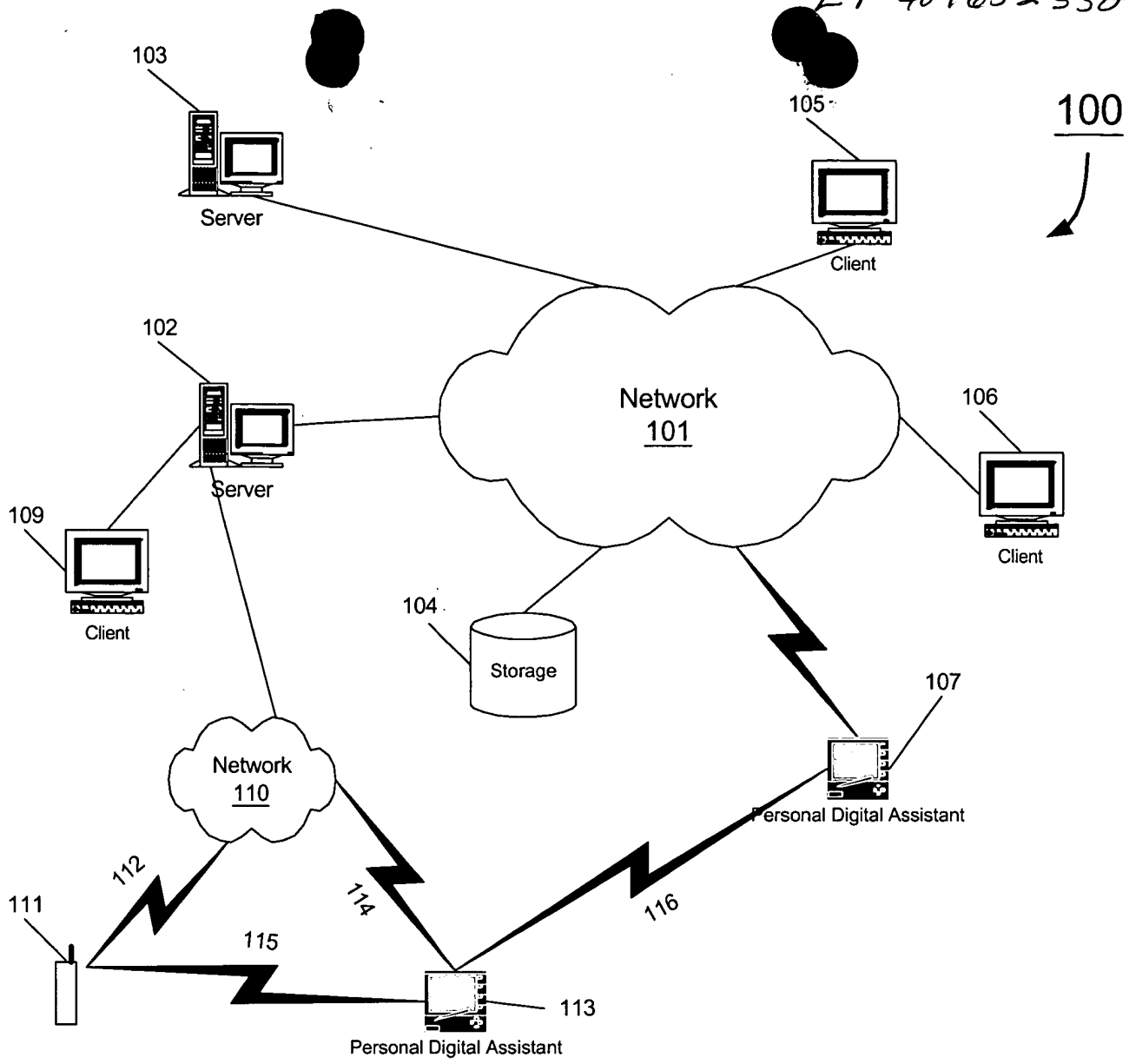
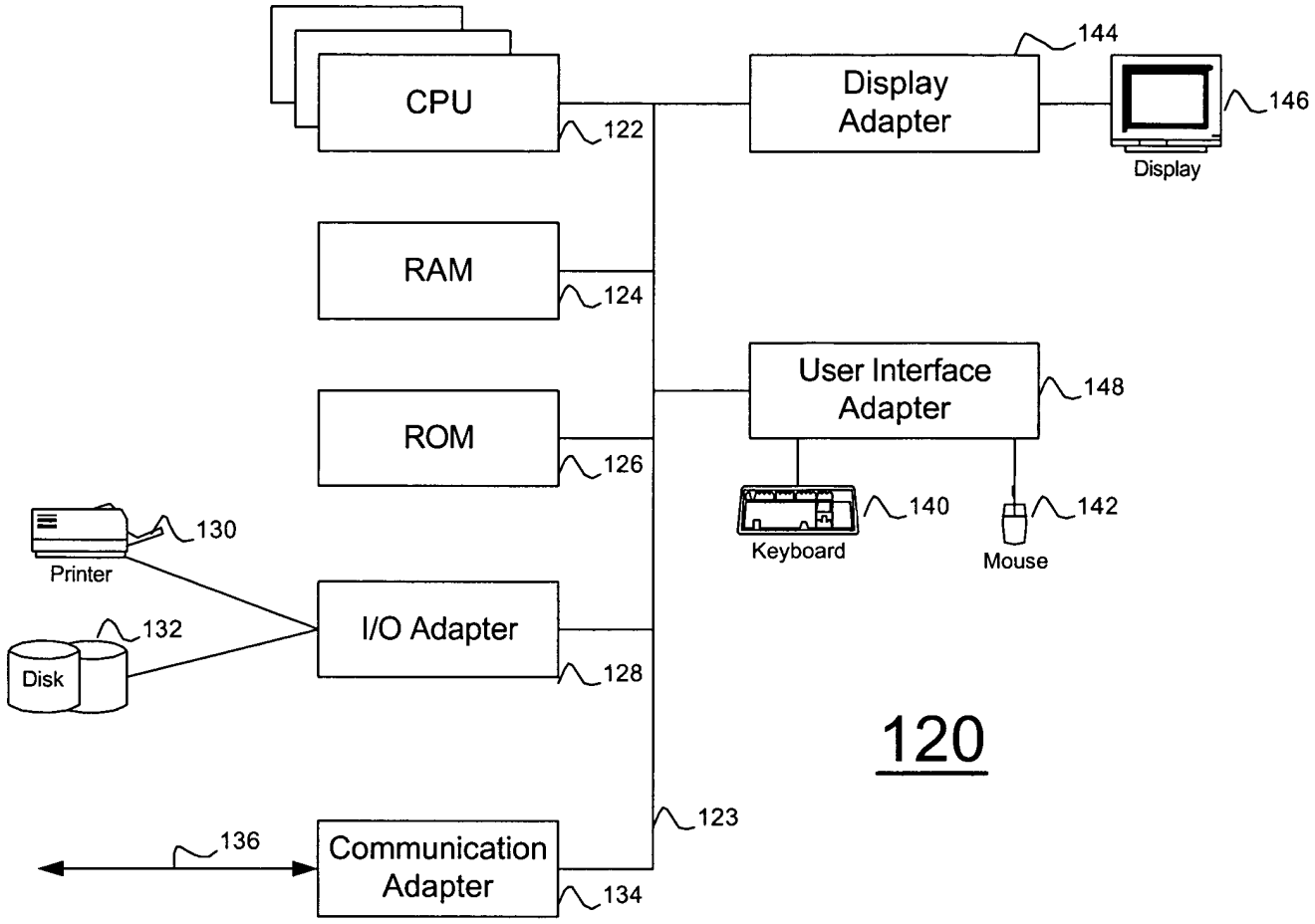
EF409652552US



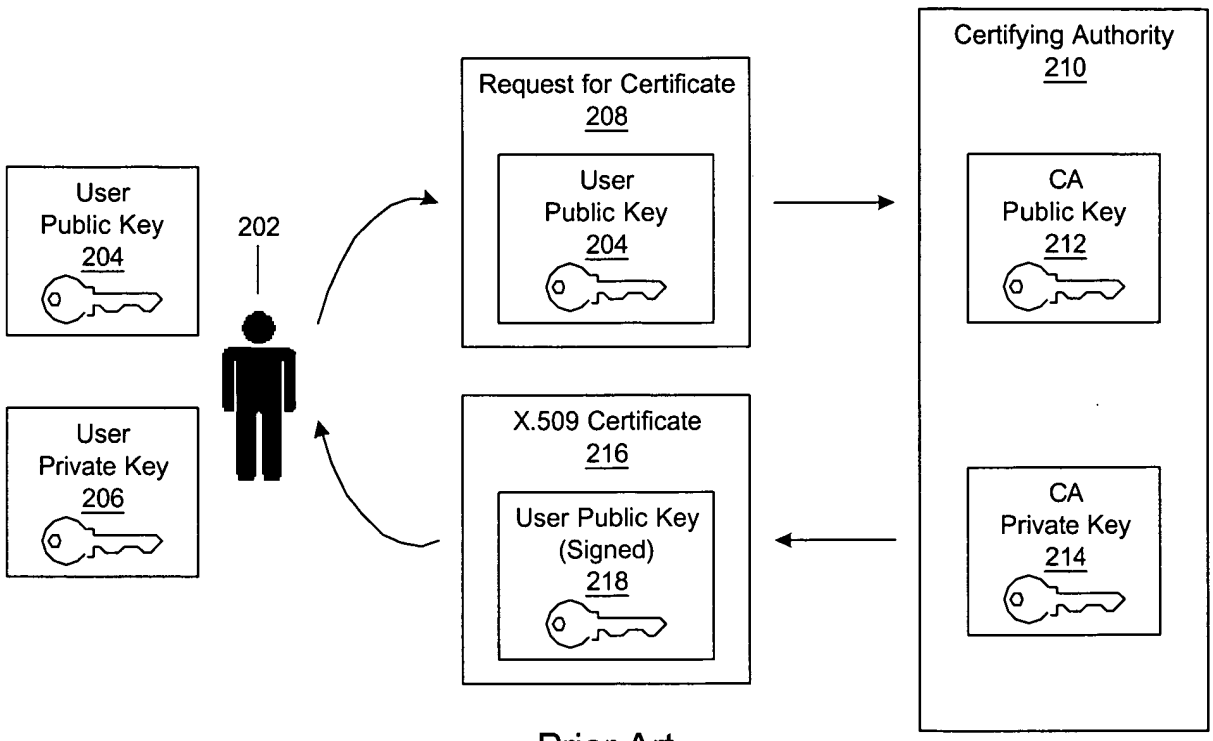

Prior Art

Figure 1A



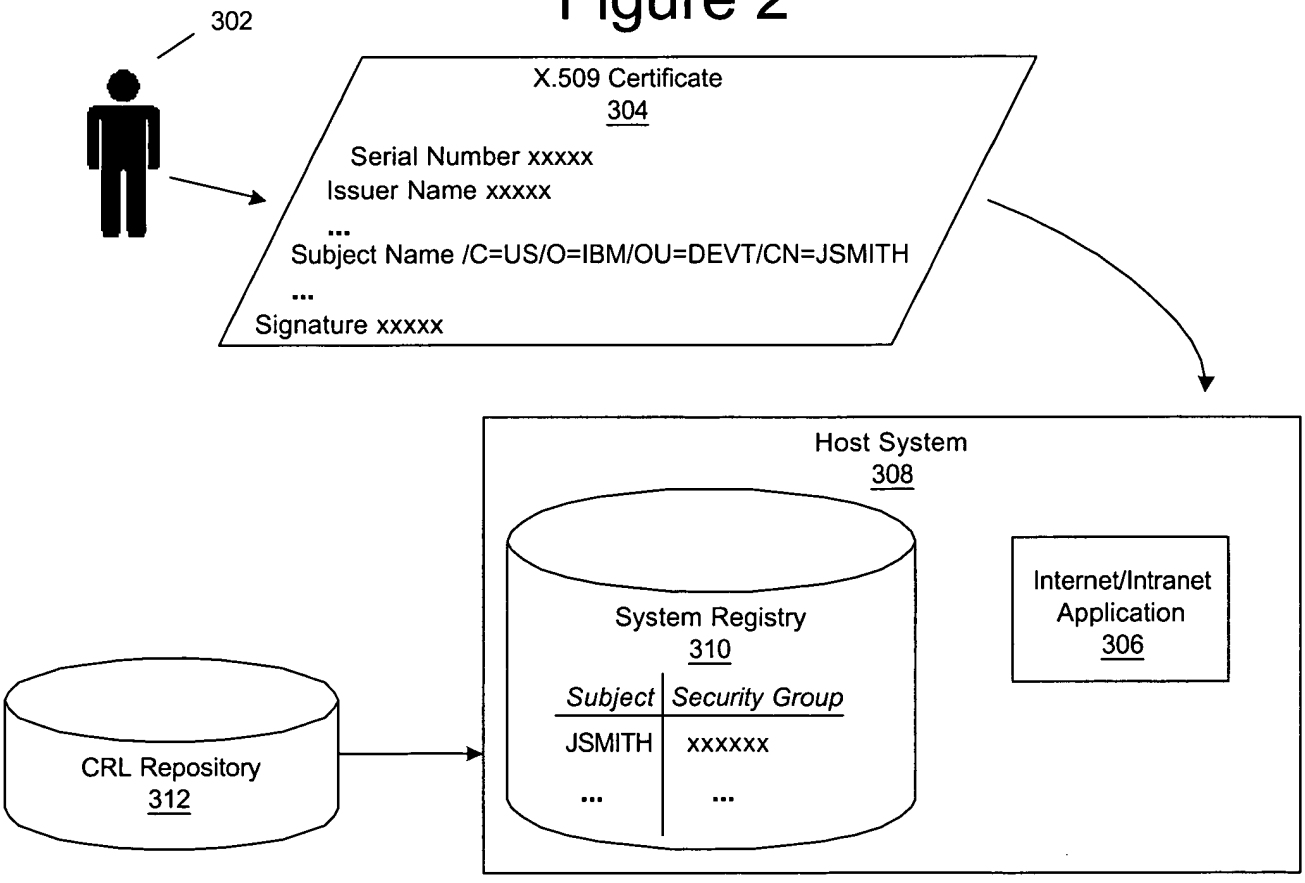

Prior Art

Figure 1B




Prior Art

Figure 2




Prior Art

Figure 3

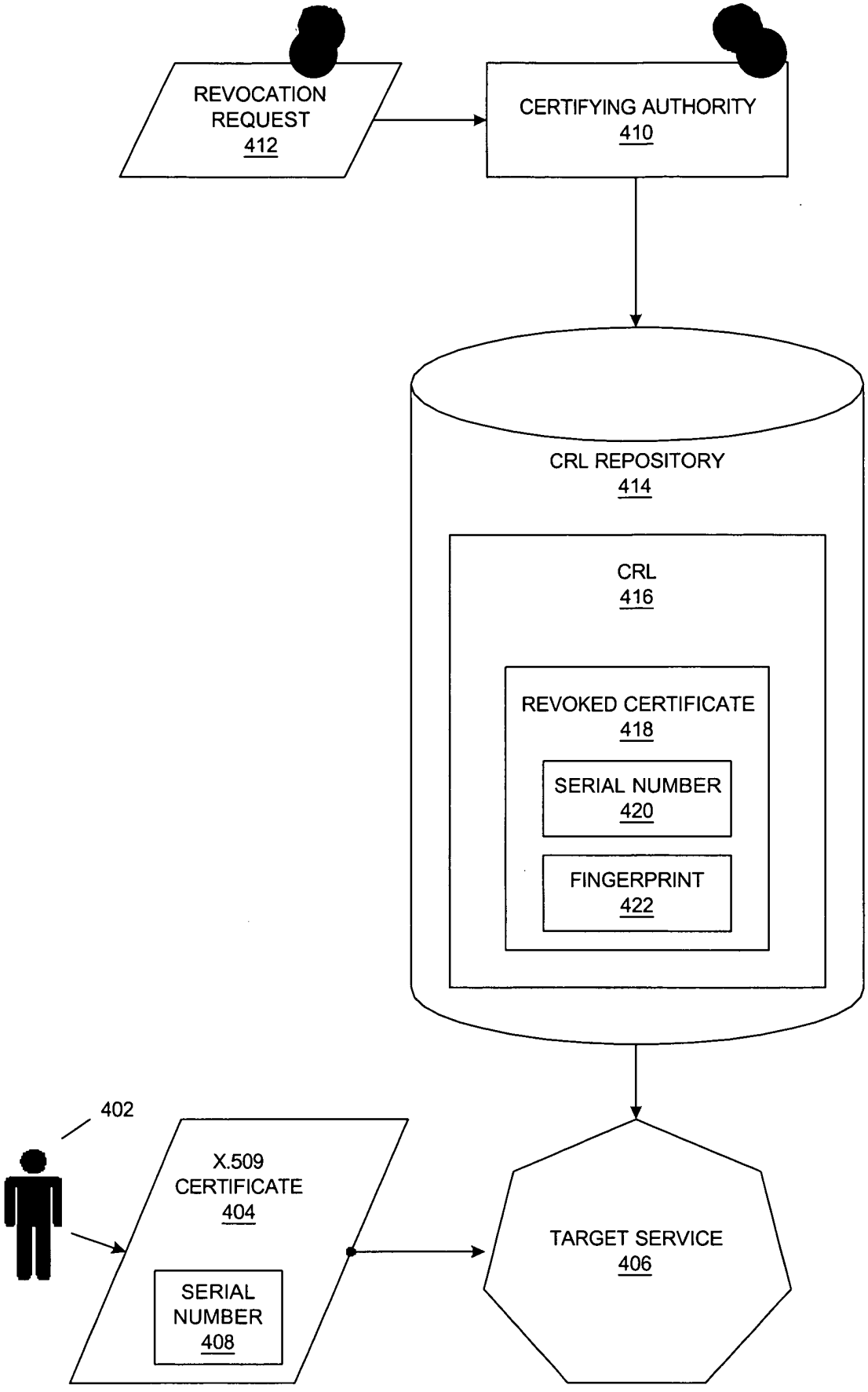

REVOCATION REQUEST 412
CERTIFYING AUTHORITY 410
CRL REPOSITORY 414
CRL 416
REVOKED CERTIFICATE 418
SERIAL NUMBER 420
FINGERPRINT 422
402
X.509 CERTIFICATE 404
SERIAL NUMBER 408
TARGET SERVICE 406

Figure 4

```
Certificate  ::=  SEQUENCE  {
      tbsCertificate              TBSCertificate,
      signatureAlgorithm          AlgorithmIdentifier,
      signature                   BIT STRING  }

TBSCertificate  ::=  SEQUENCE  {
      version           [0]     Version DEFAULT v1,
      serialNumber              CertificateSerialNumber,
      signature                 AlgorithmIdentifier,
      issuer                    Name,
      validity                  Validity,
      subject                   Name,
      subjectPublicKeyInfo      SubjectPublicKeyInfo,
      issuerUniqueID    [1]     IMPLICIT UniqueIdentifier OPTIONAL,
      subjectUniqueID   [2]     IMPLICIT UniqueIdentifier OPTIONAL,
      extensions        [3]     Extensions OPTIONAL   }

Version  ::=  INTEGER  {  v1(0), v2(1), v3(2)  }

CertificateSerialNumber  ::=  INTEGER

Validity ::= SEQUENCE {
      notBefore                 Time,
      notAfter                  Time }

Time ::= CHOICE {
      utcTime                   UTCTime,
      generalTime               GeneralizedTime }

UniqueIdentifier  ::=  BIT STRING

SubjectPublicKeyInfo  ::=  SEQUENCE  {
      algorithm                 AlgorithmIdentifier,
      subjectPublicKey          BIT STRING  }

Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension

Extension  ::=  SEQUENCE  {
      extnID                    OBJECT IDENTIFIER,
      critical                  BOOLEAN DEFAULT FALSE,
      extnValue                 OCTET STRING  }
```

Priort Art

Figure 5A

```
CertificateList ::= SEQUENCE {
        tbsCertList             TBSCertList,
        signatureAlgorithm      AlgorithmIdentifier,
        signatureValue          BIT STRING }

TBSCertList ::= SEQUENCE {
        version                 Version OPTIONAL,
        signature               AlgorithmIdentifier,
        issuer                  Name,
        thisUpdate              Time,
        nextUpdate              Time OPTIONAL,
        revokedCertificates     SEQUENCE OF SEQUENCE {
                userCertificate         CertificateSerialNumber,
                revocationDate          Time,
                crlEntryExtensions      Extensions OPTIONAL
        } OPTIONAL,
        crlExtensions   [0]     EXPLICIT Extensions OPTIONAL
}
```

Priort Art

Figure 5B

```
certFingerprint ::= SEQUENCE OF SEQUENCE {
        algorithm               AlgorithmIdentifier,
        fingerprint             octet string
}
```

Figure 6

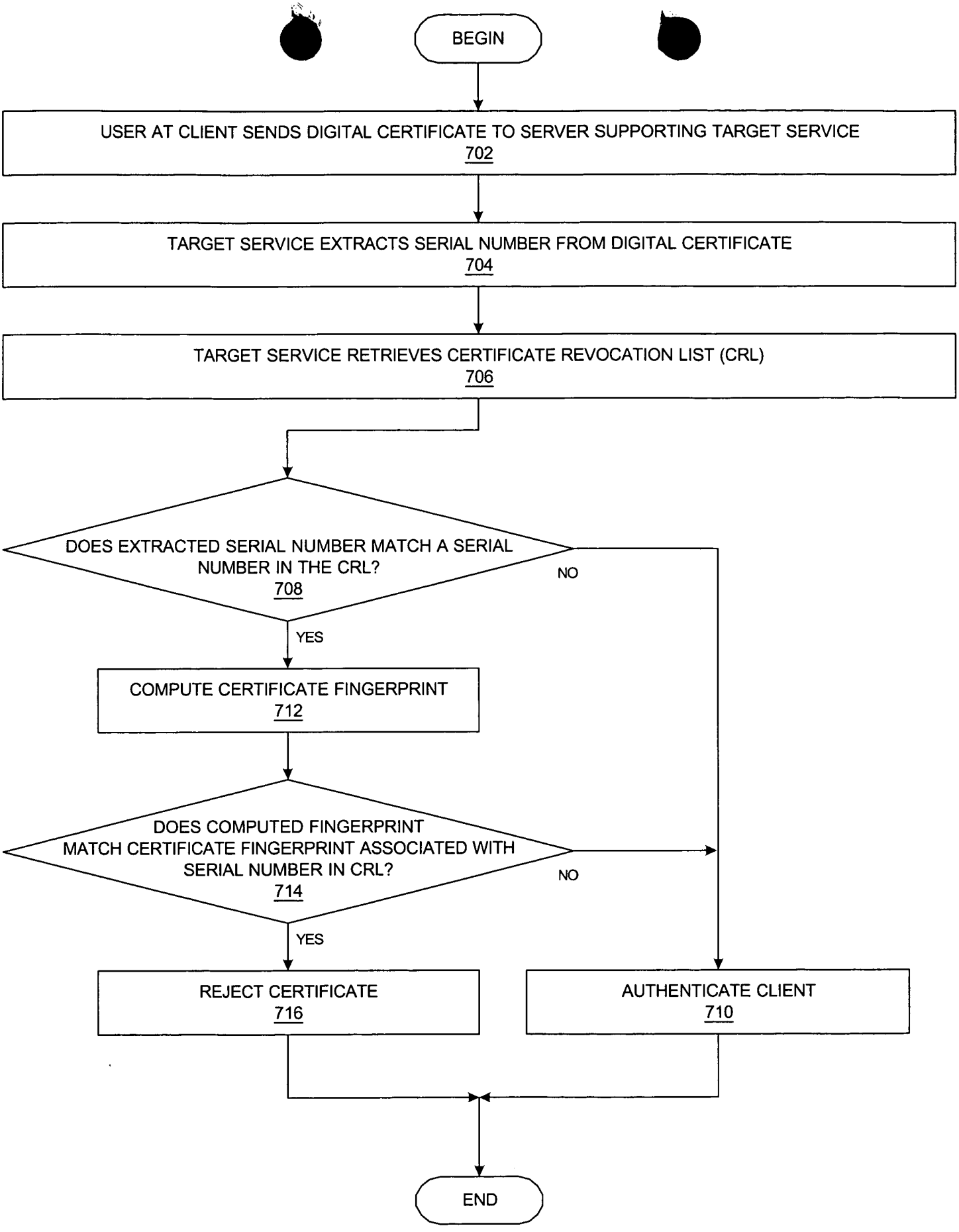

BEGIN
USER AT CLIENT SENDS DIGITAL CERTIFICATE TO SERVER SUPPORTING TARGET SERVICE
702
TARGET SERVICE EXTRACTS SERIAL NUMBER FROM DIGITAL CERTIFICATE
704
TARGET SERVICE RETRIEVES CERTIFICATE REVOCATION LIST (CRL)
706
DOES EXTRACTED SERIAL NUMBER MATCH A SERIAL NUMBER IN THE CRL?
708
NO
YES
COMPUTE CERTIFICATE FINGERPRINT
712
DOES COMPUTED FINGERPRINT MATCH CERTIFICATE FINGERPRINT ASSOCIATED WITH SERIAL NUMBER IN CRL?
714
NO
YES
REJECT CERTIFICATE
716
AUTHENTICATE CLIENT
710
END

Figure 7